AKAMAI PRODUCT BRIEF

Firewall for AI

Akamai Firewall for AI is a purpose-built security solution designed to protect AI-powered applications, large language models (LLMs), and AI-driven APIs from emerging cyberthreats. By securing inbound AI queries and outbound AI responses, the firewall closes security gaps that generative AI introduces.

With real-time detection, policy-based enforcement, and adaptive security measures, this firewall protects against prompt injections, sensitive data leaks, adversarial exploits, and AI-specific denial-of-service (DoS) attacks.

Seamlessly integrating with edge, cloud, hybrid, and on-prem environments, Firewall for AI ensures consistent security, safety, governance, and compliance while preserving performance.

AI-specific threat protection

Firewall for AI provides comprehensive security for AI-driven applications by identifying and mitigating AI-specific vulnerabilities that traditional security tools fail to address.

- **Prompt injection defense** — protects against attackers manipulating AI models through deceptive inputs.
- **Data loss prevention (DLP)** — detects and blocks sensitive data leaks in AI-generated responses, and protects against receiving sensitive data in the requests.
- **Toxic and harmful content filtering** — flags hate speech, misinformation, and offensive content before delivery.
- **Adversarial AI security** — protects against remote code execution, model backdoors, and data poisoning attacks.
- **Denial-of-service mitigation** — mitigates AI-driven DoS attacks by controlling excessive query usage and model overload.

Benefits for your business

Unified AI security posture
Standardized AI security across edge, cloud, hybrid, and on-prem

Automated AI threat detection
AI-specific protections without manual rule tuning

Seamless WAAP integration
Extends web application and API protection (WAAP) with AI defenses

Prevent AI misuse and legal risks
Blocks data leaks, IP theft, and regulatory violations

Simplified AI security
No need for in-house engineers to manually enforce security policies

Multicloud flexibility
Protects AI workloads across environments

Enterprise-grade AI protection
Backed by Akamai's global threat intelligence

Akamai

Flexible deployment options

Firewall for AI offers multiple deployment models tailored for different AI architectures and cloud environments.

Deployment model	Description
Akamai edge integration	Protects AI applications inline at the Akamai edge with low-latency security enforcement.
REST API	Scans AI inputs and outputs via API-based risk detection and scoring.
Reverse proxy deployment (roadmap capability)	Routes AI traffic through Akamai's secure proxy for deep inspection and filtering.

This flexibility allows organizations to secure LLMs deployed anywhere, including multicloud, hybrid, and on-prem environments.

How it works

AI traffic analysis

The firewall monitors and analyzes AI interactions, inspecting incoming user prompts and AI-generated outputs to detect potential threats before they reach the model or end user. By analyzing the AI query-response cycle, the firewall effectively prevents security risks while preserving application performance.

Risk scoring and adaptive threat response

AI interactions are evaluated against multiple security indicators, including prompt injections, sensitive data exposure, and adversarial exploits.

Security enforcement actions

Firewall for AI enforces three critical security measures based on risk score and customer risk appetite:

- **Monitor:** Logs detected threats for analysis without interfering with AI queries or responses.
- **Modify:** Adjusts AI-generated outputs inline, removing or altering unsafe content while maintaining a natural conversation flow.
- **Deny:** Blocks high-risk inputs from reaching the AI model and prevents unsafe responses from being returned to users.

Compliance and governance confidence

Firewall for AI can help to meet security and compliance standards. As AI-driven applications introduce new regulatory challenges, maintaining oversight of data privacy, model integrity, and security risks is critical.

Regulatory alignment

The firewall can help organizations comply with privacy, safety, and security guidelines. By enforcing AI-specific security policies, businesses can mitigate risks related to data protection regulations, ethical AI usage, and corporate governance mandates.

Security analytics and logging

Firewall for AI provides detailed audit logs and real-time security analytics, giving security teams visibility into AI security events. By monitoring query patterns, threat indicators, and response behaviors, organizations can proactively detect anomalies, enforce policy controls, and generate compliance reports.

Enterprise-grade AI protection

Backed by Akamai's global threat intelligence, the firewall continuously adapts to emerging AI security threats. By leveraging real-time data insights from AI security research and threat modeling, organizations can maintain a resilient security posture while ensuring their AI applications operate safely and responsibly.

Speak with an expert to learn more.